

18 June 1982

MEMORANDUM FOR: Executive Director
Deputy Director for Intelligence
Deputy Director for Operations
Deputy Director for Science and Technology
General Counsel
Inspector General
Comptroller

FROM: [REDACTED]
Chief, Regulations Control Division

SUBJECT: Proposed Revisions of [REDACTED] Agency Information Security
Program, and [REDACTED] Information Security Program
Handbook (Jobs #27 and 28)

FOR YOUR CONCURRENCE OR COMMENTS:

1. These proposed revisions of [REDACTED] and [REDACTED] were initiated by the Office of Information Services to update Agency information security policy and procedures to conform with changes set forth in Executive Order 12356. These proposals are to be published simultaneously with the effective date of the order, 1 August 1982; please review them on an immediate basis. Because of expeditious handling, you will find some technical editorial inconsistencies in the handbook that will be corrected at the time of printing; i.e., changing "shall" to "will" and others. We therefore ask that your attention be focused primarily on substantive content.

2. Please forward your concurrence and/or comments to the undersigned by 2 July 1982. Concurrence sheets are attached for your convenience.

Attachments:

- A. Concurrence Sheets
- B. Proposed Revision of [REDACTED]
- C. Proposed Revision of [REDACTED]

cc: AO/DCI IHSA OF
SSA/DDA OEA OL
D/OIS OP OMS
OIS/RMD ICS OS
OIS/IPD OC OTE
OIS/CRD ODP

IMMEDIATE

Form 3-65 160c

(13)

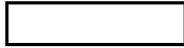
HQ. INSTRUCTION SHEET

REMOVE			INSERT			EXPLANATION
REG. NOS.	PAGE NOS.	DATE	REG. NOS.	PAGE NOS.	DATE	
	4.5& 4.6	2/24/81		4.5& 4.6		<div></div> is revised and updated to reflect policy set forth in Executive Order 12356.
Arrows in the page margin show the locations of the changes described above.						

DISTRIBUTION: AB

INFORMATION AND RECORDS MANAGEMENT

STAT



3. AGENCY INFORMATION SECURITY PROGRAM

SYNOPSIS! This regulation implements Executive
/./

Order 12356 within the Agency. It establishes the Agency program for classifying, downgrading, declassifying, marking, and safeguarding national security information.

a. INTRODUCTION

(1) Except as provided in the Atomic Energy Act of 1954, as amended, Executive Order 12356, National Security Information, provides the only basis for classifying information.

(2) The National Security Council (NSC) may review all matters concerning the implementation of Executive Order 12356, and the NSC provides overall policy direction for the executive branch information security program.

(3) The Administrator of General Services is responsible for implementing and monitoring the information security program established by the order. This responsibility is delegated to the Information Security Oversight Office (ISOO), which has a full-time director appointed by the Administrator subject to approval by the President.

(4) No Change.

(5) The D/ISOO has the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

(6) The Attorney General, upon request by the head of an agency or D/ISOO, will render an interpretation of the order with respect to any question arising in the course of its administration.

b. GENERAL

(1) No Change.

(2) This regulation establishes, effective 1 August 1982, the Agency information security program pursuant to Executive Order 12356 and related ISOO directives.

(3) & (4) No Change.

(5) A copy of this regulation and other regulations adopted to carry out this program will be submitted to the ISOO. The D/ISOO will require any regulation or guideline to be changed if it is not consistent with the order or implementing directives. Any such decision by the D/ISOO may be appealed to the NSC. The regulation or guideline will remain in effect until the appeal is decided.

(6) Unclassified regulations that establish Agency information security policy will be published in the Federal Register to the extent that these regulations affect members of the public.

(7) The D/ISOO has the authority to conduct on-site review of the Agency information security program and to require such reports, information, and other cooperation as necessary to fulfill his responsibilities. If such reports,
/ or her /

inspection, or access to specific categories of classified information would pose an exceptional national security risk, the Director of Central Intelligence may deny access. / (DCI) /
The D/ISOO may appeal such denials to the NSC. The denial will remain in effect until the appeal is decided.

c. SANCTIONS

(1) If the D/ISOO finds that a violation of E.O. 12356 or its implementing directives may have occurred, he or she ~~shall~~ make a report to the DCI or the senior Agency official designated in Section e (1) below so that corrective steps ~~if appropriate~~, may be taken. //
//, if appropriate. /

(2) Officials and employees of the Agency and Agency contractors, licensees, and grantees ~~shall~~ be subject to appropriate sanctions if they: /will/

(a) knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12356 or predecessor orders /K/

(b) knowingly and willfully classify or continue the classification of information in violation of the order or any implementing directive ~~or~~ /./

(c) knowingly and willfully violate any other provision of the order or implementing directive. /K/

(3) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and Agency regulations.

(4) The DCI or the senior Agency official designated in ~~Section c~~ (1) below ~~shall~~ ensure that appropriate and prompt corrective action is taken whenever a violation under ~~Section c~~ (2) above occurs. Either ~~shall~~ ensure that the D/ISOO is promptly notified whenever a violation under ~~Section c~~ (2) (a) or (b) occurs.

(Formerly c) d. POLICY AND PROCEDURES. No change.

(Formerly d) e. RESPONSIBILITIES

(1) The Deputy Director for Administration is the senior Agency official responsible for the direction and administration of the Agency information security program, which ~~shall~~ include an active oversight and security education program to insure effective implementation of the order ~~(Section 5.3(a))~~ As the senior official for the information security program, ~~he or she~~ is the person in the Agency other than the Director of Central Intelligence who may delegate original Top Secret classification authority.

(2) The Director of Information Services is responsible for general management of the information security program. ~~He or she~~ is the Agency focal point for contact with the ISOO. On information security program matters, ~~he or she~~ is the focal point for contact with the NSC and, through the Office of General Counsel, the Department of Justice.

(3) ~~1~~ (5) No Change.

/through/
(6) Delete.

4. Reserved.

DISTRIBUTION: AB.

TRANSMITTAL SLIP		DATE
TO: OIS/CRD		
ROOM NO. 322	BUILDING	
REMARKS:		
<p>C/S + T <u>WSS (looks good)</u> A A/C/OPS <u>AB-ok</u> Y C/ADMIN <u>M-okay</u> C A/C/INTEL <u>JE</u> M</p> <p>"he or she" is clumsy. The definition of 'he' in Webster is "used in the generic sense or when the sex of the person is unspecified". Why this paranoia based on ignorance of words ?? ?</p>		
FROM: RCD/OIS/DDA		
ROOM NO.	BUILDING	EXTENSION
	1105 Ames Bldg	

FORM NO. 241
1 FEB 55

REPLACES FORM 36-8
WHICH MAY BE USED.

(47)

STAT